Fields of Moduli of Hyperelliptic Curves

Bonnie Huggins

Abstract

Let F be an algebraically closed field with $\mathrm{char}(F) \neq 2$, let F/K be a Galois extension, and let X be a hyperelliptic curve defined over F. Let ι be the hyperelliptic involution of X. We show that X can be defined over its field of moduli relative to the extension F/K if $\mathrm{Aut}(X)/\langle\iota\rangle$ is not cyclic. We construct explicit examples of hyperelliptic curves not definable over their field of moduli when $\mathrm{Aut}(X)/\langle\iota\rangle$ is cyclic.

1 Introduction

Let X be a curve of genus g defined over a field F, let F/L be a Galois extension, and let K be the field of moduli relative the the extension F/L. (See Section 2 for the definition of "field of moduli".) It is well known that if g is 0 or 1 then X admits a model defined over K. It is also well known that if the group of automorphism of X is trivial then X can be defined over K; for example, see Example 1.7 in [6]. However, if $g \geq 2$ and $|\mathrm{Aut}(X)| > 1$, the curve X may not be definable over its field of moduli.

We examine the case where X is hyperelliptic and F is an algebraically closed field of characteristic not equal to 2. In this case $\mathrm{Aut}(X)$ is always nontrivial since it contains the hyperelliptic involution ι. Examples of hyperelliptic curves not definable over their field of moduli are given on page 177 in [8]. In [5] it is shown that X can be defined over K if $g = 2$ and $|\mathrm{Aut}(X)| > 2$. In Theorem 4.2 and Corollary 4.4 of [7] it is shown that X is definable over K if $\mathrm{char}(F) = 0$, $g \geq 2$, and $\mathrm{Aut}(X)/\langle\iota\rangle$ has at least two involutions. In Section 1 of [7] it is conjectured that X is definable over K if $\mathrm{char}(F) = 0$ and $|\mathrm{Aut}(X)| > 2$. In this paper, we refute this conjecture and show that X can be defined over K if $\mathrm{Aut}(X)/\langle\iota\rangle$ is not a cyclic group.

2 Fields of Moduli

Let K be a field, let F/K be a Galois extension and let X be a hyperelliptic curve defined over F. Let $\sigma \in \mathrm{Gal}(F/K)$. The curve ${}^{\sigma}X$ is the base

extension $X \underset{\operatorname{Spec} F}{\times} \operatorname{Spec} F$ of X by the morphism $\operatorname{Spec} F \xrightarrow{\operatorname{Spec}\sigma} \operatorname{Spec} F$. The field of moduli relative to the extension F/K is defined as the fixed field F^H of

$$H := \{\sigma \in \mathrm{Gal}(F/K) \mid X \cong {}^{\sigma}X \text{ over } F\}.$$

A subfield E of F is a field of definition for X if there exists a curve X_E defined over E such that $X \cong X_E \underset{\operatorname{Spec} E}{\times} \operatorname{Spec} F$.

Proposition 2.1. *Let K_m be the field of moduli of X. Then the subgroup H is a closed subgroup of $\mathrm{Gal}(F/K)$ for the Krull topology. That is,*

$$H = \mathrm{Gal}(F/K_m).$$

The field of K_m is contained in each field of definition between K and F (in particular, K_m is a finite extension of K). Hence if the field of moduli is a field of definition, it is the smallest field of definition between F and K. Finally, the field of moduli of X relative to the extension F/K_m is K_m.

Proof. See Proposition 2.1 in [4]. □

3 Finite Subgroups of 2-Dimensional Projective General Linear Groups

Throughout this section let $\overline{K}$ be an algebraically closed field of characteristic p with $p = 0$ or $p > 2$. In the following two lemmas we identify a matrix in $\mathrm{GL}_2(\overline{K})$ with its image in $\mathrm{PGL}_2(\overline{K})$.

Lemma 3.1. *Any finite subgroup G of $\mathrm{PGL}_2(\overline{K})$ is conjugate to one of the following groups:*

Case I: when $p = 0$ or $|G|$ is relatively prime to p.

(a) $G_{C_n} = \left\{ \begin{pmatrix} \zeta^r & 0 \\ 0 & 1 \end{pmatrix} : r = 0, 1, \ldots, n-1 \right\} \cong C_n,\ n \geq 1$

(b) $G_{D_{2n}} = \left\{ \begin{pmatrix} \zeta^r & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & \zeta^r \\ 1 & 0 \end{pmatrix} : r = 0, 1, \ldots, n-1 \right\} \cong D_{2n},\ n > 2$

(c) $G_{V_4} = \left\{ \begin{pmatrix} \pm 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & \pm 1 \\ 1 & 0 \end{pmatrix} \right\} \cong V_4 := \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

(d) $G_{A_4} = \left\{ \begin{pmatrix} \pm 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & \pm 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} i^\nu & i^\nu \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} i^\nu & -i^\nu \\ 1 & 1 \end{pmatrix}, \right.$
$\left. \begin{pmatrix} 1 & i^\nu \\ 1 & -i^\nu \end{pmatrix}, \begin{pmatrix} -1 & -i^\nu \\ 1 & -i^\nu \end{pmatrix} : \nu = 1, 3 \right\} \cong A_4$

(e) $G_{S_4} = \left\{ \begin{pmatrix} i^\nu & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & i^\nu \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} i^\nu & -i^{\nu+\nu'} \\ 1 & i^{\nu'} \end{pmatrix} : \nu, \nu' = 0,1,2,3 \right\} \cong S_4$

(f) $G_{A_5} = \left\{ \begin{pmatrix} \epsilon^r & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & \epsilon^r \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} \epsilon^r\omega & \epsilon^{r-s} \\ 1 & -\epsilon^{-s}\omega \end{pmatrix}, \begin{pmatrix} \epsilon^r\overline{\omega} & \epsilon^{r-s} \\ 1 & -\epsilon^{-s}\overline{\omega} \end{pmatrix} : r, s = 0,1,2,3,4 \right\} \cong A_5$

where $\omega = \frac{-1+\sqrt{5}}{2}$, $\overline{\omega} = \frac{-1-\sqrt{5}}{2}$, ζ *is a primitive* n^{th} *root of unity,* ϵ *is a primitive* 5^{th} *root of unity, and* i *is a primitive* 4^{th} *root of unity.*

Case II: when $|G|$ *is divisible by* p*.*

(g) $G_{\beta,A} = \left\{ \begin{pmatrix} \beta^k & a \\ 0 & 1 \end{pmatrix} : a \in A,\ k \in \mathbb{Z} \right\}$, *where* A *is a finite additive subgroup of* $\overline{K}$ *containing* 1 *and* β *is a root of unity such that* $\beta A = A$

(h) $\mathrm{PSL}_2(\mathbb{F}_{p^r})$

(i) $\mathrm{PGL}_2(\mathbb{F}_{p^r})$

where $\mathbb{F}_{p^r}$ *is the finite field with* p^r *elements.*

Proof. See §§55-58 in [10] and Chapter 3 in [9]. □

Lemma 3.2. *Let* $N(G)$ *be the normalizer of* G *in* $\mathrm{PGL}_2(\overline{K})$*. Then*

(a) $N(G_{C_n}) = \left\{ \begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & \alpha \\ 1 & 0 \end{pmatrix} : \alpha \in \overline{K}^* \right\}$ *if* $n > 1$,

(b) $N(G_{D_{2n}}) = G_{D_{4n}}$ *if* $n > 2$,

(c) $N(G_{V_4}) = G_{S_4}$,

(d) $N(G_{A_4}) = G_{S_4}$,

(e) $N(G_{S_4}) = G_{S_4}$,

(f) $N(G_{A_5}) = G_{A_5}$,

(h) $N(\mathrm{PSL}_2(\mathbb{F}_{p^r})) = \mathrm{PGL}_2(\mathbb{F}_{p^r})$, *and*

(i) $N(\mathrm{PGL}_2(\mathbb{F}_{p^r})) = \mathrm{PGL}_2(\mathbb{F}_{p^r})$.

Proof.

(a) See §55 in [10].

(b) See §55 in [10].

(c) Since G_{V_4} is a normal subgroup of G_{S_4}, $G_{S_4} \subseteq N(G_{V_4})$. Conjugation of G_{V_4} by G_{S_4} gives a homomorphism $G_{S_4} \to \mathrm{Aut}(V_4) \cong S_3$. A computation shows that the centralizer Z of G_{V_4} in $\mathrm{PGL}_2(\overline{K})$ is G_{V_4}. The kernel of this homomorphism is $Z \cap G_{S_4} = Z$. Since $G_{S_4}/Z \cong S_3$, every automorphism of G_{V_4} is given by conjugation by an element of G_{S_4}. Let $U \in N(G_{V_4})$. Then $UV \in Z = G_{V_4}$ for some $V \in G_{S_4}$, so $U \in G_{S_4}$.

(d) Since G_{V_4} is a characteristic subgroup of G_{A_4}, $N(G_{A_4}) \subseteq N(G_{V_4}) = G_{S_4}$. As G_{A_4} is normal in G_{S_4}, we get $N(G_{A_4}) = G_{S_4}$.

(e) Since G_{A_4} is a characteristic subgroup of G_{S_4}, $N(G_{S_4}) \subseteq N(G_{A_4}) = G_{S_4}$. Thus $N(G_{S_4}) = G_{S_4}$.

(f) Conjugation of G_{A_5} by $N(G_{A_5})$ gives a homomorphism $N(G_{A_5}) \to \mathrm{Aut}(A_5)$. The kernel of this homomorphism is the centralizer of G_{A_5} in $N(G_{A_5})$, which is just the centralizer Z of G_{A_5} in $\mathrm{PGL}_2(\overline{K})$. A computation shows that Z is just the identity. Since $\mathrm{Aut}(A_5)$ is finite, $N(G_{A_5})$ is a finite subgroup of $\mathrm{PGL}_2(\overline{K})$. Since $G_{A_5} \subseteq N(G_{A_5})$, by Lemma 3.1 we must have $N(G_{A_5}) = G_{A_5}$.

(h) We first show that $N(\mathrm{PSL}_2(\mathbb{F}_{p^r}))$ is finite. Conjugation of $\mathrm{PSL}_2(\mathbb{F}_{p^r})$ by $N(\mathrm{PSL}_2(\mathbb{F}_{p^r}))$ gives a homomorphism $N(\mathrm{PSL}_2(\mathbb{F}_{p^r})) \to \mathrm{Aut}(\mathrm{PSL}_2(\mathbb{F}_{p^r}))$. The kernel of this homomorphism is the centralizer Z of $\mathrm{PSL}_2(\mathbb{F}_{p^r})$ in $\mathrm{PGL}_2(\overline{K})$. A computation shows that Z is just the identity. Since $\mathrm{Aut}(\mathrm{PSL}_2(\mathbb{F}_{p^r}))$ is finite, so is $N(\mathrm{PSL}_2(\mathbb{F}_{p^r}))$. By Lemma 3.1 any finite subgroup of $\mathrm{PGL}_2(\overline{K})$ containing $\mathrm{PSL}_2(\mathbb{F}_{p^r})$ must be isomorphic to either $\mathrm{PGL}_2(\mathbb{F}_q))$ or $\mathrm{PSL}_2(\mathbb{F}_q)$ for some q. Since $SL_2(\mathbb{F}_{p^r})$ is normal in $\mathrm{GL}_2(\mathbb{F}_{p^r})$, $\mathrm{PSL}_2(\mathbb{F}_{p^r})$ is a normal subgroup of $\mathrm{PGL}_2(\mathbb{F}_{p^r})$. So $\mathrm{PGL}_2(\mathbb{F}_{p^r}) \subseteq N(\mathrm{PSL}_2(\mathbb{F}_{p^r}))$, in particular $\mathrm{PSL}_2(\mathbb{F}_{p^r})$ is strictly contained in $N(\mathrm{PSL}_2(\mathbb{F}_{p^r}))$. By the corollary on page 80 of [9], $\mathrm{PSL}_2(\mathbb{F}_q)$ is simple for $q > 3$. It follows that $N(\mathrm{PSL}_2(\mathbb{F}_{p^r})) \neq \mathrm{PSL}_2(\mathbb{F}_q)$ for $q \geq 3$. By Theorem 9.9 on page 78 of [9], the only nontrivial normal subgroup of $\mathrm{PGL}_2(\mathbb{F}_q)$ is $\mathrm{PSL}_2(\mathbb{F}_q)$ if $q > 3$. Therefore $N(\mathrm{PSL}_2(\mathbb{F}_{p^r})) = \mathrm{PGL}_2(\mathbb{F}_{p^r})$.

(i) Clear from the proof of the previous case.

□

4 Isomorphisms of Hyperelliptic Curves

Throughout this section let K be a perfect field of characteristic p with $p = 0$ or $p > 2$ and let X be a hyperelliptic curve defined over an algebraic closure $\overline{K}$ of K with K as its field of moduli. In particular, X admits a degree-2 morphism to $\mathbb{P}^1$ and the genus of X is at least 2. Each element of $\mathrm{Aut}(X)$ induces an automorphism of $\mathbb{P}^1$ fixing the branch points. The number of branch points is ≥ 3 (in fact ≥ 6), so $\mathrm{Aut}(X)$ is finite. We get a homomorphism $\mathrm{Aut}(X) \to \mathrm{Aut}(\mathbb{P}^1) = \mathrm{PGL}_2(\overline{K})$ with kernel generated by the hyperelliptic involution ι. Let $G \subset PGL_2(\overline{K})$ be the image of this homomorphism. Replacing the original map $X \to \mathbb{P}^1$ by its composition with an automorphism $g \in \mathrm{Aut}(\mathbb{P}^1) = \mathrm{PGL}_2(\overline{K})$ has the effect of changing G to gGg^{-1}, so we may assume that G is one of the groups listed in Lemma 3.1. Fix an equation $y^2 = f(x)$ for X where $f \in \overline{K}[x]$ and $\mathrm{disc}(f) \neq 0$. So the function field $\overline{K}(X)$ equals $\overline{K}(x, y)$.

Proposition 4.1. *Let X be as above and let X' be a hyperelliptic curve defined over $\overline{K}$ given by $y^2 = f'(x)$, where $f'(x)$ is another squarefree polynomial in $\overline{K}[x]$. Every isomorphism $\varphi\colon X \to X'$ is given by an expression of the form:*

$$(x, y) \mapsto \left(\frac{ax + b}{cx + d}, \frac{ey}{(cx + d)^{g+1}} \right),$$

for some $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\overline{K})$ and $e \in \overline{K}^*$. The pair (M, e) is unique up to replacement by $(\lambda M, e\lambda^{g+1})$ for $\lambda \in \overline{K}^*$. If $\varphi'\colon X' \to X''$ is another isomorphism, given by (M', e'), then the composition $\varphi'\varphi$ is given by $(M'M, e'e)$.

Proof. See Proposition 2.1 in [1]. ☐

Let $\Gamma = \mathrm{Gal}(\overline{K}/K)$ and let $\sigma \in \Gamma$. Then ${}^{\sigma}X$ is the smooth projective model of $y^2 = f^{\sigma}(x)$, where $f^{\sigma}(x)$ is the polynomial obtained from $f(x)$ by applying σ to the coefficients.

Lemma 4.2. *Following the notation used above, let $\sigma \in \Gamma$ and suppose that $\varphi\colon X \to {}^{\sigma}X$ is given by (M, e). Let $\overline{M}$ be the image of M in $\mathrm{PGL}_2(\overline{K})$. If $G \neq G_{\beta,A}$ then $\overline{M}$ is in the normalizer $N(G)$ of G in $\mathrm{PGL}_2(\overline{K})$. If $G = G_{\beta,A}$ then M is an upper triangular matrix.*

Proof. Since $\mathrm{Aut}({}^{\sigma}X) = \{\psi^{\sigma} \mid \psi \in \mathrm{Aut}(X)\}$, the group of automorphisms of $\mathbb{P}^1$ induced by $\mathrm{Aut}({}^{\sigma}X)$ is $G^{\sigma} := \{U^{\sigma} \mid U \in G\}$.

Let ψ be an automorphism of X given by (V, v). Since ψ is an automorphism, $V \in \mathrm{GL}_2(\overline{K})$ is a lift of some element $\overline{V} \in G$. Then $\varphi\psi\varphi^{-1}$ is an automorphism of ${}^{\sigma}X$ given by (MVM^{-1}, v). We have $\overline{MVM^{-1}} = \overline{M}\ \overline{V}\ \overline{M}^{-1} \in G^{\sigma}$. It follows that $\overline{M}G\overline{M}^{-1} = G^{\sigma}$. If $G \neq G_{\beta,A}$, by Lemma 3.1, $G^{\sigma} = G$. So $\overline{M} \in N(G)$. If $G = G_{\beta,A}$, then since G^{σ} has an elementary abelian subgroup of the same form as G, a simple computation shows that M is an upper triangular matrix. □

Lemma 4.3. *Following the above notation, suppose that for every $\tau \in \Gamma$ there exists an isomorphism $\varphi_{\tau} \colon X \to {}^{\tau}X$ given by (M_{τ}, e) where $\overline{M}_{\tau} \in G^{\tau}$. Then X can be defined over K.*

Proof. Let $P_1, \ldots, P_n$ be the hyperelliptic branch points of $X \to \mathbb{P}^1$. Let $\tau \in \Gamma$. The isomorphism $\varphi_{\tau} \colon X \to {}^{\tau}X$ induces an isomorphism on the canonical images $\mathbb{P}^1 \to \mathbb{P}^1$ which is given by $\overline{M}_{\tau}$. Then $\overline{M}_{\tau}$ sends $\{P_1, \ldots, P_n\}$ to $\{\tau(P_1), \ldots, \tau(P_n)\}$. Since $\overline{M}_{\tau} \in G^{\tau}$ it merely permutes the set $\{P_1, \ldots, P_n\}$. Since τ is arbitrary we have

$$\prod_{P_i \neq \infty} (x - P_i) \in K[x].$$

It follows that X can be defined over K. □

Corollary 4.4. *Suppose that $N(G) = G$ and $G \neq G_{\beta,A}$. Then X can be defined over K.*

Proof. By Lemma 3.1, $G^{\sigma} = G$ for all $\sigma \in \Gamma$. Let $\tau \in \Gamma$. By Lemma 4.2, any isomorphism $X \to {}^{\tau}X$ is given by (M, e) where $\overline{M} \in N(G) = G = G^{\tau}$.

□

5 The Main Result

The following two results of Dèbes and Emsalem will be used in the proof of our main result. They rely on the notions of a cover and the field of moduli of a cover, for which we refer the reader to § 2.4 in [3].

Theorem 5.1. *Let F/K be a Galois extension and X be a hyperelliptic curve defined over F with K as field of moduli. Let $B = X/\operatorname{Aut}(X)$. Then there exists a model B_K of the curve $B = X/\operatorname{Aut}(X)$ defined over K such that the cover $X \to B$ with K-base B_K is of field of moduli K.*

Proof. See Theorem 3.1 in [4]. The authors make the additional assumption that $\mathrm{char}(K)$ does not divide $|\operatorname{Aut}(X)|$ but do not use it in their proof. □

Corollary 5.2. *Suppose that F is algebraically closed. If B_K has a K-rational point, then K is a field of definition of X.*

Proof. It suffices to show that the cover $X \to B$ with K-base B_K can be defined over K, since a field of definition of the cover is automatically a field of definition of X. By Theorem 5.1, the field of moduli of the cover $X \to B$ with K-base B_K is K. If K is a finite field then $\mathrm{Gal}(F/K)$ is a projective profinite group. In this case, by Corollary 3.3 of [3] the cover $X \to B$ can be defined over K. If K is not a finite field then since $B_K \cong_K \mathbb{P}^1_K$, B_K has a rational point off the branch point set of $X \to B_K \times F$. Then by Corollary 3.4 and § 2.9 of [3], the cover can be defined over K. ☐

The curve B_K is called the canonical model of $X/\operatorname{Aut}(X)$ over the field of moduli of X. Let $\Gamma = \mathrm{Gal}(F/K)$. In the proof of Theorem 5.1, Dèbes and Emsalem show the canonical model exists by using the following argument. For all $\sigma \in \Gamma$ there exists an isomorphism $\varphi_\sigma \colon X \to {}^\sigma X$ defined over F. Each induces an isomorphism $\tilde{\varphi_\sigma} \colon X/\operatorname{Aut}(X) \to {}^\sigma X/\operatorname{Aut}({}^\sigma X)$ that makes the following diagram commute:

$$\begin{tikzcd} X \arrow[r, "\varphi_\sigma"] \arrow[d, "\rho"'] & {}^\sigma X \arrow[d, "\rho^\sigma"] \\ X/\operatorname{Aut}(X) \arrow[r, "\tilde{\varphi_\sigma}"'] & {}^\sigma X/\operatorname{Aut}({}^\sigma X) \end{tikzcd}$$

Composing $\tilde{\varphi_\sigma}$ with the canonical isomorphism

$$i_\sigma \colon {}^\sigma X/\operatorname{Aut}({}^\sigma X) \to {}^\sigma(X/\operatorname{Aut}(X))$$

we obtain an isomorphism

$$\overline{\varphi_\sigma} \colon X/\operatorname{Aut}(X) \to {}^\sigma(X/\operatorname{Aut}(X)).$$

The family $\{\overline{\varphi_\tau}\}_{\tau\in\Gamma}$ satisfy Weil's cocycle condition $\overline{\varphi_\tau}^\sigma\,\overline{\varphi_\sigma} = \overline{\varphi_{\sigma\tau}}$ given in Theorem 1 of [11]. This shows that B_K exists.

Let $F(B)$ be the function field of B. Since $B \cong \mathbb{P}^1$, $F(B) = F(t)$ for some element t. We use t as a coordinate on B. Suppose that $\overline{\varphi_\sigma}$ is given by

$$t \mapsto \frac{at+b}{ct+d}.$$

Define $\sigma^* \in \operatorname{Aut}(F(t)/K)$ by

$$\sigma^*(t) = \frac{at+b}{ct+d},\ \sigma^*(\alpha) = \sigma(\alpha),\ \alpha \in F.$$

One can verify that $(\sigma\tau)^*(w) = \sigma^*(\tau^*(w))$ for all $w \in F(t)$. So we get a homomorphism $\Gamma \to \mathrm{Aut}(F(B)/K)$, $\sigma \mapsto \sigma^*$. The curve B_K is the variety over K corresponding to the fixed field of $\Gamma^* = \{\sigma^*\}_{\sigma\in\Gamma}$.

The following lemma will be used in the proof of the main theorem.

Lemma 5.3. *Let L/K be a field extension of odd degree. Let C be a curve of genus 0 defined over K and suppose that $C(L) \neq \varnothing$. Then $C(K) \neq \varnothing$.*

Proof. Let $P \in C(L)$ and let $n = [L : K]$. Let $\tau_1, \ldots, \tau_n$ be the distinct embeddings of L into an algebraic closure of L. Then $D = \Sigma\tau_i(P)$ is a divisor of degree n defined over K. Let ω be a canonical divisor on C. Since $\deg(\omega) = -2$, we can take a linear combination of D and ω to obtain a divisor D' of degree 1. Since $\deg(\omega - D') < 0$, by the Riemann-Roch theorem $l(D') > 0$. So there exists an effective divisor D'' linearly equivalent to D' defined over K. Since D'' is effective and of degree 1 it consists of a point in $C(K)$. ☐

Theorem 5.4. *Let K be a field of characteristic not equal to 2. Let X be a hyperelliptic curve defined over $\overline{K}$, an algebraic closure of K. Let G =Aut$(X)/\langle\iota\rangle$ where ι is the hyperelliptic involution of X. Suppose that G is not cyclic or that G is cyclic of order divisible by the characteristic of K. Then X can be defined over its field of moduli relative to the extension $\overline{K}/K$.*

Proof. Let $\Gamma = \mathrm{Gal}(\overline{K}/K)$. By Proposition 2.1 we may assume that K is the field of moduli of X. By Proposition 4.1 we may assume that G is given by one of the groups in Lemma 3.1. Fix an equation $y^2 = f(x)$ for X where $f \in \overline{K}[x]$ and $\mathrm{disc}(f) \neq 0$. So the function field $\overline{K}(X)$ equals $\overline{K}(x, y)$. There are eight cases.

(b) $G \cong D_{2n}$, $n > 2$. The function field of $X/\mathrm{Aut}(X)$ equals the subfield of $\overline{K}(X)$ fixed by $G_{D_{2n}}$ acting by fractional linear transformations. Then $t := x^n + x^{-n}$ is fixed by $G_{D_{2n}}$ and is a rational function of degree $2n$ in x, so the function field of $X/\mathrm{Aut}(X)$ equals $\overline{K}(t)$. Therefore we use t as coordinate on $X/\mathrm{Aut}(X)$. The map $\rho\colon X \to X/\mathrm{Aut}(X)$ is given by $(x, y) \mapsto (x^n + x^{-n})$. Let $\sigma \in \Gamma$. By Lemmas 4.2 and 3.2, $\varphi_\sigma\colon X \to {}^\sigma X$ is given by (M, e) where $\overline{M} \in D_{4n}$. Then the map $\rho^\sigma\varphi_\sigma\colon X \to {}^\sigma X/\mathrm{Aut}({}^\sigma X)$ is given by $(x, y) \mapsto \pm(x^n + x^{-n})$. So $\sigma^*(t) = \pm t$. The curve B_K corresponds to the fixed field of $\overline{K}(t)$ under Γ^*. Then $t = 0$ corresponds to a point $P \in B_K(K)$.

(c) $G \cong V_4$. The element $t := x^2+x^{-2}$ is fixed by G_{V_4} and is a rational function of degree 4 in x. So the function field of $X/\mathrm{Aut}(X)$ equals $\overline{K}(t)$.

We use t as a coordinate on $X/\operatorname{Aut}(X)$. The map $\rho\colon X \to X/\operatorname{Aut}(X)$ is given by $(x, y) \mapsto (x^2 + x^{-2})$. Let $\sigma \in \Gamma$. By Lemmas 4.2 and 3.2, $\varphi_\sigma\colon X \to {}^\sigma X$ is given by (M, e) where $\overline{M} \in G_{S_4}$. A computation shows that $\sigma^*(t)$ is one of the following:

i. t

ii. $-t$

iii. $\frac{2t+12}{t-2}$

iv. $\frac{2t-12}{-t-2}$

v. $\frac{2t-12}{t+2}$

vi. $\frac{2t+12}{-t+2}$.

Since $\overline{\varphi}_\tau\colon X/\operatorname{Aut}(X) \to {}^\tau(X/\operatorname{Aut}(X))$ is defined over K for all $\tau \in \Gamma$, we have $\overline{\varphi_\tau}\,\overline{\varphi_\sigma} = \overline{\varphi_{\sigma\tau}}$ for all $\tau \in \Gamma$. The fractional linear transformations i through vi form a group under composition isomorphic to S_3. The map $\tau \mapsto \tau^*(t)$ defines a homomorphism from Γ to this group. The kernel of this homomorphism is $\Lambda := \{\tau \in \Gamma \mid \tau^*(t) = t\}$. So $|\Gamma/\Lambda| = 1, 2, 3$, or 6.

Case 1: $|\Gamma/\Lambda| = 1$. In this case the fixed field of Γ^* is $K(t)$ and $B_K = \mathbb{P}^1_K$.

Case 2: $|\Gamma/\Lambda| = 2$. Let σ be a representative of the nontrivial coset. There are three cases.

i. $\sigma^*(t) = -t$. Then $t = 0$ corresponds to a point $P \in B_K(K)$.

ii. $\sigma^*(t) = \frac{2t+12}{t-2}$. Then $t = 6$ corresponds to a point $P \in B_K(K)$.

iii. $\sigma^*(t) = \frac{2t-12}{-t-2}$. Then $t = -6$ corresponds to a point $P \in B_K(K)$.

Case 3: $|\Gamma/\Lambda| = 3$. Since the fixed field of Λ^* is $\overline{K}^\Lambda(t)$, B_K has a $\overline{K}^\Lambda$-rational point. By Lemma 5.3, since $[\overline{K}^\Lambda : K]$ is odd, B_K has a K-rational point.

Case 4: $|\Gamma/\Lambda| = 6$. Let Π be a subgroup of Γ containing Λ such that Π/Λ is a subgroup of Γ/Λ of order 2. By Case 2, B_K has a $\overline{K}^\Pi$ rational point. Since $[\overline{K}^\Pi : K] = 3$ is odd, by Lemma 5.3, B_K has a K-rational point.

(d) $G \cong A_4$. The element $t' := x^2 + x^{-2}$ is fixed by the normal subgroup G_{V_4}. From (c), we see that the element

$$t := \frac{1}{4}t'\left(\frac{2t'-12}{t'+2}\right)\left(\frac{2t'+12}{-t'+2}\right) = \frac{x^{12} - 33x^8 - 33x^4 + 1}{-x^{10} + 2x^6 - x^2}$$

is fixed by G_{A_4} and is a rational function of degree 12 in x. So the function field of $X/\operatorname{Aut}(X)$ equals $\overline{K}(t)$. We use t as coordinate on $X/\operatorname{Aut}(X)$. The map $\rho\colon X \to X/\operatorname{Aut}(X)$ is given by

$$(x, y) \mapsto (x^{12} - 33x^8 - 33x^4 + 1)/(-x^{10} + 2x^6 - x^2).$$

Let $\sigma \in \Gamma$. By Lemmas 4.2 and 3.2, $\varphi_\sigma\colon X \to {}^\sigma X$ is given by (M, e) where $\overline{M} \in G_{S_4}$. A computation shows that $\sigma^*(t) = \pm t$. Then $t = 0$ corresponds to a point $P \in B_K(K)$.

(e) $G \cong S_4$. By Lemma 3.2, $N(G) = G$. So by Corollary 4.4, X can be defined over K.

(f) $G \cong A_5$. By Lemma 3.2, $N(G) = G$. So by Corollary 4.4, X can be defined over K.

(g) $G = G_{\beta,A}$. Let d be the order of β and let $t = g(x) := \prod_{\alpha \in A}(x - \alpha)^d$. Then t is a rational function of degree $|G|$ fixed by $G_{\beta,A}$ acting by fractional linear transformations. So the function field of $X/\operatorname{Aut}(X)$ equals $\overline{K}(t)$. We use t as a coordinate function of $X/\operatorname{Aut}(X)$. Let $\sigma \in \Gamma$. By Lemma 4.2, $\varphi_\sigma\colon X \to {}^\sigma X$ is given by (M, e) where M is an upper diagonal matrix. So $\sigma^*(t) = g^\sigma(ax + b)$ for some $a \neq 0$ and b. Let P be the point of $X/\operatorname{Aut}(X)$ corresponding to $x = \infty$. Then since $g^\sigma(a\infty + b) = g(\infty)$, P corresponds to a point in $B_K(K)$.

(h) $G = \operatorname{PSL}_2(\mathbb{F}_{p^r})$. Let $q = p^r$. It can be deduced from Theorem 6.21 on page 409 of [9] that $\operatorname{PSL}_2(\mathbb{F}_q)$ is generated by the image in $\operatorname{PGL}_2(\overline{K})$ of the following matrices

$$\left\{ \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} : a \in \mathbb{F}_{p^r} \right\}.$$

Let

$$g(x) = \frac{((x^q - x)^{q-1} + 1)^{\frac{q+1}{2}}}{(x^q - x)^{\frac{q^2-q}{2}}}.$$

One can verify that $g(\frac{-1}{x}) = g(x)$ and $g(x + a) = g(x)$ for all $a \in \mathbb{F}_{p^r}$. Since g is a rational function of x of degree $\frac{q^3-q}{2} = |\operatorname{PSL}_2(\mathbb{F}_q)|$, the function field of $X/\operatorname{Aut}(X)$ is $\overline{K}(t)$ where $t = g(x)$. We use t as a coordinate function on $X/\operatorname{Aut}(X)$. The map $\rho\colon X \to X/\operatorname{Aut}(X)$ is given by

$$(x, y) \mapsto \frac{((x^q - x)^{q-1} + 1)^{\frac{q+1}{2}}}{(x^q - x)^{\frac{q^2-q}{2}}}.$$

Let $\sigma \in \Gamma$. By Lemmas 4.2 and 3.2, $\varphi_\sigma \colon X \to {}^\sigma X$ is given by (M, e) where $\overline{M} \in \mathrm{PGL}_2(\mathbb{F}_q)$. A computation shows that $\sigma^*(t) = \pm t$. Then $t = 0$ corresponds to a point $P \in B_K(K)$.

(i) $G = \mathrm{PGL}_2(\mathbb{F}_{p^r})$. By Lemma 3.2, $N(G) = G$. So by Corollary 4.4, X can be defined over K.

□

Specific examples of hyperelliptic curves not definable over their field of moduli are given on page 177 of [8]; these examples have $|G| = 1$. Adjusting these examples, we now construct others with $|G| > 5$.

Let $n > 5$, let m be odd, and consider the polynomial $f(x) \in \mathbb{C}[x]$ given by

$$f(x) = a_0 x^{nm} + \sum_{r=1}^{m} (a_r x^{n(m+r)} + (-1)^r a_r^c x^{n(m-r)}),$$

with $a_m = 1$, $a_0 \in \mathbb{R}^*$, and where z^c is the complex conjugate of z for any $z \in \mathbb{C}$. Assume that for $r = 1, \ldots, m-1$ we have $a_r \neq (-1)^r \beta^{-nr} a_r^c$ for any $2mn^{th}$ root of unity β and that $f(x)$ is square free.

Lemma 5.5. *Following the above notation, let X by the hyperelliptic curve over $\mathbb{C}$ given by $y^2 = f(x)$. Let ι be the hyperelliptic involution of X and let ν be the automorphism of X defined by $\nu(x, y) = (\zeta x, y)$, where ζ is a primitive n^{th} root of unity. Then* $\mathrm{Aut}(X) = \langle \iota \rangle \oplus \langle \nu \rangle$.

Proof. Let $G = \mathrm{Aut}(X)/\langle \iota \rangle$. The image of ν in G under the quotient map $\mathrm{Aut}(X) \to G$ has order n. Since $n > 5$, by Lemma 3.1, G is either cyclic or dihedral. In either case the image of ν in G generates a cyclic normal subgroup of G.

Suppose that G is cyclic of order $n' > n$. Since the only elements in $\mathrm{PGL}_2(\mathbb{C})$ that commute with the image of diagonal matrices are the images of diagonal matrices, by Lemma 4.1 there exists an element $u \in \mathrm{Aut}(X)$ defined by

$$u(x, y) = (\zeta' x, ey)$$

where $e \in \mathbb{C}^*$ and ζ' is a primitive $(n')^{th}$ root of unity. It follows that $f(\zeta' x)$ is a scalar multiple of $f(x)$. This is a contradiction by our choice of coefficients for f.

Suppose that G is dihedral. By Lemma 3.2 (a) and Lemma 4.1, there exists an element $v \in \mathrm{Aut}(X)$ defined by

$$v(x, y) = (\alpha/x, e'y/x^{mn})$$

where e', $\alpha \in \mathbb{C}^*$. It follows that $x^{2mn}f(\alpha/x)$ is a scalar multiple of $f(x)$. Since

$$x^{2mn}f(\alpha/x) = \alpha^{nm}(a_0 x^{nm} + \sum_{r=1}^{m}((-1)^r \alpha^{-nr} a_r^c x^{n(m+r)} + \alpha^r a_r x^{n(m-r)})$$

and $a_0 \neq 0$, we must have $\frac{x^{2mn}}{\alpha^{nm}} f(\alpha/x) = f(x)$. Since $a_m = 1$, we must have $\alpha^{mn} = -1$ and $a_r = (-1)^r \alpha^{-nr} a_r^c$ for $r = 1, \ldots, m-1$. This is a contradiction. Therefore G is cyclic of order n.

The function field of X is $\mathbb{C}(x, y)$ and the function field of $X/\operatorname{Aut}(X)$ is $\mathbb{C}(x^n)$. Since the places in $\mathbb{C}(x^n)$ corresponding to $x^n = 0$ and $x^n = \infty$ do not ramify completely in $\mathbb{C}(x, y)$, by Theorem 5.1 of [2] we have $\operatorname{Aut}(X) = \langle \iota \rangle \oplus \langle \nu \rangle$. □

Proposition 5.6. *Following the above notation, let X by the hyperelliptic curve of genus $g = mn - 1$ over $\mathbb{C}$ given by $y^2 = f(x)$. The field of moduli of X relative to the extension $\mathbb{C}/\mathbb{R}$ is $\mathbb{R}$ and is not a field of definition for X.*

Proof. By Lemma 5.5, $\operatorname{Aut}(X) = \langle \iota \rangle \oplus \langle \nu \rangle$ where ι is the hyperelliptic involution of X, and $\nu(x, y) = (\zeta x, y)$ where ζ is a primitive n^{th} root of unity. The map μ defined by

$$\mu(x, y) = ((\omega x)^{-1}, i x^{-nm} y),$$

where $\omega^n = -1$, is an isomorphism between the curve X and the complex conjugate curve ${}^cX$. Any isomorphism $X \to {}^cX$ is given by $\mu\nu^k$, or $\mu\iota\nu^k$ for some $0 \leq k \leq n-1$. We have $\mu\iota = \iota\mu$,

$$\mu\nu(x, y) = ((\omega\zeta x)^{-1}, i(\zeta x)^{-nm} y) = \nu^c \mu(x, y),$$

and

$$\mu^c\mu(x, y) = ((\omega^{-1}(\omega x)^{-1})^{-1}, -i(\omega x)^{nm}(i x^{-nm} y)) = (\omega^2 x, -y) = \nu^l \iota(x, y)$$

for some l. Then

$$(\mu\nu^k)^c \mu\nu^k = \mu^c \nu^{-k} \mu\nu^k = \mu^c \mu \nu^{2k} = \iota\nu^{2k+l} \neq Id$$

and

$$(\mu\iota\nu^k)^c \mu\iota\nu^k = \mu^c \iota\nu^{-k} \mu\iota\nu^k = \mu^c \mu \nu^{2k} = \iota\nu^{2k+l} \neq Id.$$

Therefore Weil's cocycle condition from Theorem 1 of [11] does not hold. So X cannot be defined over $\mathbb{R}$. □

Acknowledgements

The author learned of the conjecture of [7] from Bjorn Poonen, and thanks him for comments on an early draft of this paper. The author was partially supported by NSF grant DMS-0301280 of Bjorn Poonen.

References

[1] Matthew Baker, Enrique Gonzalez-Jimenez, Josep Gonzalez, and Bjorn Poonen, *Finiteness results for modular curves of genus at least 2*, arXiv:math.NT/0211394, November 2002.

[2] Rolf Brandt and Henning Stichtenoth, *Die Automorphismengruppen hyperelliptischer Kurven*, Manuscripta Math. **55** (1986), no. 1, 83–92.

[3] Pierre Dèbes and Jean-Claude Douai, *Algebraic covers: field of moduli versus field of definition*, Ann. Sci. École Norm. Sup. (4) **30** (1997), no. 3, 303–338.

[4] Pierre Dèbes and Michel Emsalem, *On fields of moduli of curves*, J. Algebra **211** (1999), no. 1, 42–56.

[5] J. Quer G. Cardona, *Field of moduli and field of definition for curves of genus 2*, arXiv:math.NT/0207015, June 2002.

[6] Bernhard Köck, *Belyi's theorem revisited*, Beiträge Algebra Geom. **45** (2004), no. 1, 253–265.

[7] T. Shaska, *Computational aspects of hyperelliptic curves*, Computer mathematics. Proceedings of the sixth Asian symposium (ASCM 2003), Beijing, China, April 17-19, 2003, Lecture Notes Series on Computing, vol. 10, World Sci. Publishing, River Edge, NJ, 2003, pp. 248–257.

[8] Goro Shimura, *On the field of rationality for an abelian variety*, Nagoya Math. J. **45** (1972), 167–178.

[9] Michio Suzuki, *Group theory. I*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 247, Springer-Verlag, Berlin, 1982, Translated from the Japanese by the author.

[10] Heinrich Weber, *Lehrbuch der Algebra*, vol. II, Vieweg, Braunschweig, 1896.

[11] André Weil, *The field of definition of a variety*, Amer. J. Math. **78** (1956), 509–524.

Department of Mathematics, University of California, Berkeley, CA 94720
E-mail address: bhuggins@math.berkeley.edu